1990.69815 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re U.S. Patent Application)
)
Applicant: Tsuneki Takahashi)
)
Serial No.)
)
Filed: February 23, 2004)
)
For: MAGNETIC DISK APPARATUS,)
CIPHER PROCESSING METHOD)
AND PROGRAM)
)
Art Unit:)

I hereby certify that this paper is being deposited with the United States Postal Service as EXPRESS MAIL in an envelope addressed to: Mail Stop PATENT APPLICATION, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this date.

February 23, 2004 *Express Mail Label No.: EV032731633US*
Date

CLAIM FOR PRIORITY

Mail Stop PATENT APPLICATION
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicants claim foreign priority benefits under 35 U.S.C. § 119 on the basis of the foreign application identified below:

Japanese Patent Application No. 2003-136867, filed May 15, 2003.

A certified copy of the priority document is enclosed.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

By
Patrick G. Burns
Registration No. 29,367

Customer No. 24978

February 23, 2004
300 South Wacker Drive
Suite 2500
Chicago, Illinois 60606
Phone: (312) 360-0080
Fax: (312) 360-9315
P:\DOCS\0113\69646\438182.DOC

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　５月１５日

出願番号
Application Number: 特願２００３－１３６８６７

[ST. 10/C]: ［ＪＰ２００３－１３６８６７］

出願人
Applicant(s): 富士通株式会社

２００３年１２月１５日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３１０４００９

【書類名】　特許願
【整理番号】　0350393
【提出日】　平成15年 5月15日
【あて先】　特許庁長官殿
【発明の名称】　磁気ディスク装置、暗号処理方法及びプログラム
【請求項の数】　5
【国際特許分類】　G11B 5/09
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　高橋　常樹
【特許出願人】
【識別番号】　000005223
【氏名又は名称】　富士通株式会社
【代理人】
【識別番号】　100079359
【弁理士】
【氏名又は名称】　竹内　進
【手数料の表示】
【予納台帳番号】　009287
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9704823
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　磁気ディスク装置、暗号処理方法及びプログラム

【特許請求の範囲】

【請求項1】

データの暗号化と復元に使用する暗号鍵を記憶した暗号鍵記憶部と、

インタフェースを介して上位装置から入力されたデータを前記暗号鍵を用いて暗号化して記録媒体に記録させる暗号エンコード部と、

前記記録媒体から読み出された暗号データを前記暗号鍵を用いて復元して前記インタフェースより上位装置にデータを出力させる暗号デコード部と、

前記暗号鍵記憶部に記憶されている暗号鍵を変更する暗号鍵変更部と、

を備えたことを特徴とする磁気ディスク装置。

【請求項２】

請求項1記載の磁気ディスク装置に於いて、前記暗号鍵変更部は、前記記録媒体上のユーザ記録領域に存在する全ての記録データを一括して破棄する際に、前記暗号鍵記憶部に記憶されている暗号鍵を変更することを特徴とする磁気ディスク装置。

【請求項３】

請求項1記載の磁気ディスク装置に於いて、前記暗号鍵変更部は、上位装置のコマンド体系以外の特殊コマンドにより、前記暗号鍵記憶部の暗号鍵を変更することを特徴とする磁気ディスク装置。

【請求項４】

磁気ディスク装置の暗号処理方法に於いて、

データの暗号化と復号に使用する暗号鍵を記憶部に記憶する暗号鍵記憶ステップと、

インタフェースを介して上位装置から入力されたデータを前記暗号鍵を用いて暗号データに変換して記録媒体に記録させる暗号化記録ステップと、

前記記録媒体から読み出された暗号データを前記暗号鍵を用いて復元して前記インタフェースより上位装置にデータを出力させる復元読出ステップと、

前記暗号鍵儀記憶部に記憶されている暗号鍵を変更する暗号鍵変更ステップと、

を備えたことを特徴とする磁気ディスク装置の暗号処理方法。

【請求項５】

磁気ディスク装置に内蔵されたコンピュータに、

データの暗号化と復号に使用する暗号鍵を記憶部に記憶する暗号鍵記憶ステップと、

インタフェースを介して上位装置から入力されたデータを前記暗号鍵を用いて暗号データに変換して記録媒体に記録させる暗号化記録ステップと、

前記記録媒体から読み出された暗号データを前記暗号鍵を用いて復元して前記インタ暗号鍵記憶部に記憶されている暗号鍵を変更する暗号鍵変更ステップと、

を実行させることを特徴とするプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンピュータを廃棄する際に媒体記録データを喪失させる磁気ディスク装置、暗号処理方法及びプログラムに関し、特に暗号処理を利用して媒体記録データを喪失させる磁気ディスク装置、暗号処理方法及びプログラムに関する。

【０００２】

【従来の技術】

従来、使用していたコンピュータを廃棄したり、再利用する場合、磁気ディス

ク装置に記録されているデータの流出を防ぐ必要がある。

【０００３】

このような磁気ディスク装置のデータの流出を防ぐ方法としては、データを消去する方法、暗号化データを記録する方法、磁気ディスク装置を物理的に破壊する方法が考えられる。

【０００４】

【特許文献１】

特開２００１－０９２７１９号

【０００５】

【発明が解決しようとする課題】

しかしながら、このような従来の磁気ディスク装置のデータの流出を防ぐ方法は次のような問題点がある。

【０００６】

まず磁気ディスク装置のデータ消去には、磁気ディスク装置から完全にデータが消去する場合と、後のデータ復旧を考えＯＳから見えなくするだけで、データそのものは磁気ディスク装置から消去されない場合がある。

【０００７】

しかし、ユーザからはこのようなデータ消去の違いを把握することは難しく、ＯＳから見えなくしただけのデータ消去の場合、データの流出が発生する問題が考えられる。またデータを完全に消去する場合、近年の磁気ディスク装置の大容量化に伴い、全データを消去するのに時間がかかる問題がある。

【０００８】

また磁気ディスク装置のデータを暗号化する場合、データと暗号鍵が別々に扱われるため、データが流出しても復元ができないため安全である。しかし、磁気ディスク装置はコンピュータの起動に多用されており、ＯＳまで暗号化することは困難である。

【０００９】

即ち、磁気ディスク装置に記録するＯＳを含む全データを暗号化した場合には

、コンピュータ側に磁気ディスク装置から読み出した暗号データを復元するＯＳに依存しない専用の暗号復元機能をファームウェア等により設ける必要があり、暗号復元機能をもたないコンピュータでは利用できない。

【００１０】

また磁気ディスク装置のデータを暗号化する場合、データと暗号鍵が別々に扱われるため、ユーザに暗号鍵の管理の負担を強いる問題がある。

【００１１】

更に、磁気ディスク装置を物理的に破壊する方法は、データの流出を確実に防ぐ事ができるが、動作可能な装置を破壊することになり、装置の再利用が不可能となりコスト的に問題がある。

【００１２】

本発明は、暗号化技術を利用して簡単且つ確実にデータ流出を防止する磁気ディスク装置、暗号処理方法及びプログラムを提供することを目的とする。

【００１３】

【課題を解決するための手段】

図１は本発明の原理説明図である。本発明の磁気ディスク装置は、データの暗号化と復元に使用する暗号鍵４２を記憶した暗号鍵記憶部５０と、インタフェースを介して上位装置から入力されたデータを暗号鍵４２を用いて暗号化して記録媒体に記録させる暗号エンコード部５４と、記録媒体から読み出された暗号データを暗号鍵４２を用いて復元してインタフェースより上位装置にデータを出力させる暗号デコード部５６と、暗号鍵記憶部５０に記憶されている暗号鍵４２を変更する暗号鍵変更部５８とを備えたことを特徴とする。

【００１４】

本発明の磁気ディスク装置では、記録媒体に記録されているデータは暗号化されているため、本発明の磁気ディスク装置を廃棄及び転用する際には、暗号鍵を変更する。このように暗号鍵が変更されると、媒体に記録されている暗号データは変更前の暗号鍵で暗号化されたデータであり、変更後の暗号鍵で復元しても正しいデータは復元されず、無意味なデータが復元されるだけである。このため磁

気ディスク装置に保持している暗号鍵の変更という簡単な操作で、記録領域の全面消去を行うことなく、ＯＳを含む記録領域の全データを破棄することかできる。

【００１５】

また本発明の磁気ディスク装置は、データの暗号化及び復元は磁気ディスク装置内で行うため、インタフェースを介したデータは従来の磁気ディスク装置と同じであり、コンピュータ側はＯＳを含む全てのデータを従来の磁気ディスク装置と同様に扱うことができる。このためコンピュータ側は専用の暗号処理機能を必要としない。

【００１６】

また本発明の磁気ディスク装置は、暗号化されたデータと暗号鍵を装置内に格納して運用するため、ユーザは通常の使用では暗号鍵の管理する必要がない。ユーザは、本発明の磁気ディスク装置を廃棄及び転用の際に暗号鍵の変更を行うだけであり、ユーザの暗号鍵の管理に伴う負担を軽減する。

【００１７】

更に、本発明の磁気ディスク装置は、データの破棄は暗号鍵の変更によって行うため、暗号鍵を変更した後も装置の機能は失われず、暗号鍵の変更によって磁気ディスク装置は未使用状態に戻り、コンピュータの再利用のためＯＳのインストールから始めることで、コンピュータを未使用装置として再利用できる。

【００１８】

ここで、暗号鍵格納部は、装置の製造段階で書き込まれた所定の暗号鍵を記憶する。暗号鍵記憶部は不揮発メモリを使用する。また、暗号鍵記憶部は記録媒体のユーザ記録領域以外の記録領域としても良い。

【００１９】

暗号鍵変更部は、記録媒体上のユーザ記録領域に存在する全ての記録データを一括して破棄する際に、暗号鍵記憶部に記憶されている暗号鍵を変更する。暗号鍵変更部は、上位装置のコマンド体系以外の特殊コマンドにより、暗号鍵記憶部の暗号鍵を変更する。この特殊コマンドはＯＳに依存しないため、運用中に誤って暗号鍵が変更されることを防止する。

【００２０】

暗号鍵変更部は、上位装置にインストールされた暗号鍵変更アプリケーションからの特殊コマンドにより、暗号鍵記憶部の暗号鍵を変更する。また暗号鍵変更部は、上位装置がネットワークを介してインストールした暗号鍵変更アプリケーションからの特殊コマンドにより、暗号鍵記憶部の暗号鍵を変更する。

【００２１】

このため磁気ディスク装置のデータを破棄する際には、ＦＤ等のリムーバル媒体あるいは製造メーカのホームページの参照で提供されるアプリケーションを使用して磁気ディスク装置内の暗号鍵を変更することができ、ユーザにおける暗号鍵の管理は一切不要となる。

【００２２】

暗号鍵変更部は、装置内における物理的なイベント操作を認識して、暗号鍵記憶部の暗号鍵を変更する。このように装置内のディップスイッチの操作、特定のピンに対する信号入力、ジャンパ線の切断などの操作を認識して暗号鍵の変更を行うこともできる。

【００２３】

暗号鍵変更部は、暗号鍵記憶部に記憶されている暗号鍵の掻き混ぜ処理（シャッフル処理）等より新たな暗号鍵を生成して変更する。また暗号鍵変更部は、暗号鍵記憶部に記憶されている暗号鍵を、上位装置からの暗号鍵変更コマンドに付加された別の暗号鍵に変更するようにしても良い。

【００２４】

本発明は、磁気ディスク装置の暗号処理方法を提供する。この暗号処理方法は、

データの暗号化と復号に使用する暗号鍵を記憶部に記憶する暗号鍵記憶ステップと、

インタフェースを介して上位装置から入力されたデータを暗号鍵を用いて暗号データに変換して記録媒体に記録させる暗号化記録ステップと、

記録媒体から読み出された暗号データを暗号鍵を用いて復元してインタフェースより上位装置にデータを出力させる復元読出ステップと、

暗号鍵記憶部に記憶されている暗号鍵を変更する暗号鍵変更ステップと、
を備えたことを特徴とする。

【００２５】

ここで暗号鍵変更ステップは、記録媒体上のユーザ記録領域に存在する全ての記録データを一括して破棄する際に、暗号鍵記憶部に記憶されている暗号鍵を変更する。

【００２６】

本発明は、磁気ディスク装置に内蔵されたコンピュータで実行されるプログラムを提供する。このプログラムは、磁気ディスク装置内蔵のコンピュータに、

データの暗号化と復号に使用する暗号鍵を記憶部に記憶する暗号鍵記憶ステップと、

インタフェースを介して上位装置から入力されたデータを暗号鍵を用いて暗号データに変換して記録媒体に記録させる暗号化記録ステップと、

記録媒体から読み出された暗号データを暗号鍵を用いて復元してインタフェースより上位装置にデータを出力させる復元読出ステップと、

暗号鍵記憶部に記憶されている暗号鍵を変更する暗号鍵変更ステップと、
を実行させることを特徴とする。

【００２７】

ここで、暗号鍵変更ステップは、記録媒体上のユーザ記録領域に存在する全ての記録データを一括して破棄する際に、暗号鍵記憶部に記憶されている暗号鍵を変更する。

【００２８】

なお、これ以外の暗号処理方法及びプログラムの詳細は、磁気ディスク装置の装置構成の場合と基本的に同じになる。

【００２９】

【発明の実施の形態】

図２は、本発明の暗号処理が適用される磁気ディスク装置のブロック図である。図２において、磁気ディスク装置としてのハードディスクドライブ（ＨＤＤ）

１０は、ディスクエンクロージャ１２とコントロールボード１４で構成される。ディスクエンクロージャ１２にはスピンドルモータ１６が設けられ、スピンドルモータ１６の回転軸に磁気ディスク媒体２０－１，２０－２を装着し、一定速度で回転させる。

【００３０】

またディスクエンクロージャ１２にはボイスコイルモータ１８が設けられ、ボイスコイルモータ１８はヘッドアクチュエータのアームの先端にヘッド２２－１～２２－４を搭載しており、磁気ディスク２０－１，２０－２の記録面に対するヘッドの位置決めを行う。尚、ヘッド２２－１～２２－４にはライトヘッドとリードヘッドが一体化されて搭載されている。

【００３１】

ヘッド２２－１～２２－４はヘッドＩＣ２４に対し信号線接続されており、ヘッドＩＣ２４は上位装置となるホスト１１からのライトコマンドまたはリードコマンドに基づく、ヘッドセレクト信号で書込または読出しを行ういずれかひとつのヘッドを選択する。またヘッドＩＣ２４にはライト系については書込アンプが設けられ、リード系についてはプレアンプが設けられている。

【００３２】

コントロールボード１４にはリードライトＬＳＩ２６，ハードディスクコントローラ（ＨＤＣ）２８，ホストインタフェース３０，ＳＤＲＡＭ３２，ＭＰＵ３４，フラッシュＲＯＭ３６，ＶＣＭ／ＳＰＭコントローラ３８が設けられている。これに加え本発明にあってはコントロールボード１４に暗号処理部４０を新たに設けている。

【００３３】

また暗号処理部４０で使用される暗号鍵４２をこの実施形態にあっては、不揮発メモリであるフラッシュＲＯＭ３６に記憶している。フラッシュＲＯＭ３６に対する暗号鍵４２の記録は磁気ディスク装置１０の製造段階で特殊なコマンドを使用して行われる。

【００３４】

ここで磁気ディスク装置１０の動作を簡単に説明すると次のようになる。ホス

ト１１からライトコマンドとライトデータをホストインタフェース３０で受けると、ライトコマンドをＭＰＵ３４で解読し、必要に応じて転送バッファとして機能するＳＤＲＡＭ３２のバッファリングを含めて受信したライトデータをハードディスクコントローラ２８で所定のファーマットデータに変換すると共に、ＥＣＣ符号を付加し、リードライトＬＳＩ２６のライト系でスクランブル、ＲＬＬ符号変換、更に書込位相補償を行った後、ヘッドＩＣ２４を介して選択したヘッドのライトヘッドから磁気ディスクに書き込む。

【００３５】

この時、ＭＰＵ３４からＶＣＭ／ＳＰＭコントローラ３８にヘッド位置決め信号が与えられており、ボイスコイルモータ１８よりヘッドをコマンドで指示された位置に位置決めしている。

【００３６】

一方、リード動作はヘッドＩＣ２４のヘッドセレクトで選択されたリードヘッドから読み出された読出信号をリードライトＬＳＩ２６に入力し、パーシャルレスポンス最尤検出（ＰＲＭＬ）によりリードデータを復調した後、ハードディスクコントローラ２８でＥＣＣ処理を行ってエラーを検出訂正をした後、転送バッファとしてのＳＤＲＡＭ３２のバッファリングを介してホストインタフェース３０からリードデータをホスト１１に転送する。

【００３７】

このような磁気ディスク装置１０におけるライトデータの書込み及びリードデータの読出しにつき本発明にあっては、ホストインタフェース３０の前段にハードウェアまたはファームウェアの機能により実現される暗号処理部４０を新たに設けている。

【００３８】

暗号処理部４０はホストインタフェース３０で受信したライトデータをハードディスクコントローラ２８に転送する際に、フラッシュＲＯＭ３６に記憶されている暗号鍵４２の鍵コード「ａ１～ａｎ」を使用してライトデータを暗号化し、暗号化されたデータをハードディスクコントローラ２８でフォーマッティングした後にＥＣＣ符号を付加し、リードライトＬＳＩ２６，ヘッドＩＣ２４を介して

、そのとき選択されているリードヘッドから磁気ディスクに書き込む。

【００３９】

一方、磁気ディスク装置から読み出された信号については、ハードディスクコントローラ２８より接続される暗号化されているリードデータを暗号処理部４０に入力し、フラッシュＲＯＭ３６に記憶している暗号鍵４２の鍵コード「ａ１～ａｎ」を使用して暗号データを復号し、復号したリードデータをホストインタフェース３０を介してホスト１１に転送する。

【００４０】

図３は、本発明に適用される磁気ディスク装置の他の実施形態であり、この実施形態にあっては暗号化処理をプログラムにより実行することを特徴とする。即ち図３の実施形態にあっては、図２のハードディスクコントローラ２８とホストインタフェース３０の間に設けていた暗号処理部４０が取り除かれており、その代わりＭＰＵ３４にプログラムの実行により実現される暗号処理部４０を設けている。

【００４１】

このようなＭＰＵ３４の暗号処理部４０にあっても、ホストインタフェース３０からのライトデータをハードディスクコントローラ２８より受けてフラッシュＲＯＭ３６の暗号鍵４２のキーコード「ａ１～ａｎ」により暗号化してライト系を介して磁気ディスクに書き込む。

【００４２】

また磁気ディスクより書き込まれた暗号化されているリードデータについてはハードディスクコントローラ２８から出力する際にＭＰＵ３４に設けた暗号処理部４５によりフラッシュＲＯＭ３６の暗号鍵４２の鍵コード「ａ１～ａｎ」を使用して暗号を復元し、復元されたリードデータをホストインタフェース３０を介してホスト１１に転送する。

【００４３】

このように本発明の磁気ディスク装置にあっては、図２にように暗号処理部４０をハードウェアで構成するか、図３のように暗号処理部４０をプログラムで構成するかは必要に応じて適宜に定めることができる。

【００４４】

図４は、本発明の暗号処理部４０の機能構成のブロック図である。この暗号処理部４０の機能構成は、図２のハードウェアの構成については回路部の機能として実現され、また図３のプログラムの場合にはプログラムの処理機能として実現される。

【００４５】

図４において、暗号化処理部４０はホストインタフェース３０とライトデータ処理部４６及びリードデータ処理部４８の間に設けられている。ここでライトデータ処理部４６は図２及び図３のハードディスクコントローラ２８及びリードライトＬＳＩ２６のライト系をまとめたものであり、一方、リードデータ処理部４８は同じくリードライトＬＳＩ２６とハードディスクコントローラ２８におけるリード系をまとめたものである。

【００４６】

暗号処理部４０は、暗号鍵記憶部５０，暗号鍵設定部５２，暗号エンコード部５４，暗号デコード部５６及び暗号鍵変更部５８を備える。暗号鍵記憶部５０はこの実施形態にあっては、図２及び図３に示した不揮発メモリとしてのフラッシュＲＯＭ３６で実現され、磁気ディスク装置の製造段階に特殊コマンドにより暗号鍵４２として鍵コード「ａ１～ａｎ」が予め記憶されている。

【００４７】

暗号エンコード部５４はホストインタフェース３０を介してホスト１１から入力されたライトデータを暗号鍵設定部５２により設定された暗号鍵記憶部５０の暗号鍵４２を用いて暗号化し、暗号化されたライトデータをライトデータ処理部４６から磁気ディスク媒体に記憶する。

【００４８】

暗号デコード部５６は磁気ディスク媒体から読み出されたリードデータ処理部４８で復唱された暗号化されたリードデータを入力し、暗号鍵設定部５２により設定される暗号鍵記憶部５０より読み出された暗号鍵４２を使用してデータを復元し、ホストインタフェース３０から上位ホスト１１に復号されたリードデータを転送させる。

【００４９】

更に暗号鍵変更部５８は本発明の磁気ディスク装置１０を搭載したホスト１１を廃棄する際に、磁気ディスク装置上のユーザー記憶領域に存在する記憶データを一括して廃棄するために暗号鍵記憶部５０に記憶している暗号鍵４２の鍵コード「ａ１～ａｎ」を別の鍵コード「ｂ１～ｂｎ」を持つ暗号鍵に変更する。

【００５０】

この実施形態にあっては暗号鍵変更部５８はホスト１１側から転送される暗号鍵変更のための特殊コマンドをホストインタフェース３０を介して受けることで暗号鍵記憶部５０の暗号鍵４２の変更を実行する。

【００５１】

暗号鍵変更部５８に対するホスト１１からの暗号鍵変更のための特殊コマンドは、例えば本発明の磁気ディスク装置の製造段階で使用する特殊なコマンドであり、ホスト１１のＯＳに依存することがなく、従って運用中においてホストのＯＳからのコマンドによって暗号鍵記憶部５０の暗号鍵４２の変更されることはない。

【００５２】

ここで本発明の暗号処理部４０で使用する暗号としては、例えば次のようなものがある。

【００５３】

（１）ＤＥＳ

ＤＥＳ暗号は1977年にアメリカ商務省標準局（ＮＢＳ）がデータ暗号化規格（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）を公募したときにＩＢＭ（Ｒ）から提出された方式に修正が加えられたものである。ＤＥＳ暗号は、データを１ブロック６４ビットとして扱い、暗号鍵は７バイトの鍵データと１バイトの奇数パリティから成り立っている。

【００５４】

（２）ＣＡＳＴ－１２８

ＣＡＳＴ－１２８暗号は、エントラスト・テクノロジー社（Ｅｎｔｒｕｓｔ Ｔｅｃｈｎｏｌｏｇｉｅｓ）のカルロス・アダムス（Ｃａｒｌｉｓｌｅ Ａｄａ

ｍｓ）とスタッフォード・トラバース（Ｓｔａｆｆｏｒｄ　Ｔｒａｖａｒｓｅｓ）によって開発されたブロック暗号である。ブロック長は６４ビット、鍵長は１～１２８ビット可変となっており、１２～１６ラウンドで処理される。このアルゴリズムには特許が成立しているが、フリーで使用できることが明言されており、ＲＦＣ２１４４として公開されている。

【００５５】

（３）その他、ＩＳＯ／ＩＥＣ　９９７９に登録されている暗号アルゴリズム

本発明の暗号処理部４０にあっては前述した暗号のアルゴリズムをそのまま適用しても良いし、暗号鍵変更部５８でライトデータにランダムな冗長を付加した後に、例えばＤＥＳアルゴリズムなどにより暗号化し、リードデータについては暗号デコード部５６でＤＥＳアルゴリズムなどで復号した後に冗長分を切り捨ててデータを出力しても良い。

【００５６】

このようにデータを暗号化する際にランダムな冗長を付加することで暗号が万一解読された場合にも冗長データで無意味なデータとなっていることで安全性を更に高めることができる。

【００５７】

図５は、図４の暗号処理部４０による処理手順を示したフローチャートである。このフローチャートは図３のＭＰＵ３４に設けている暗号処理部４４を実現するプログラムの処理手順を同時に表している。この暗号処理の手順は本発明の磁気ディスク装置のパワーオンスタートにより実行され、次の処理手順からなる。

【００５８】

ステップＳ１：暗号鍵記憶部となる不揮発メモリから予め記憶されている暗号鍵の鍵コード「ａ１～ａｎ」を読み出して暗号エンコード部５４と暗号デコード部５６に設定する。

ステップＳ２：ライトアクセスをチェックし、ホスト１１からライトコマンド及びライトデータが転送されるライトアクセスであればステップＳ３に進み、そうでければステップＳ４に進む。

ステップＳ３：ライトデータを暗号鍵の鍵コード「ａ１～ａｎ」により暗号デー

タに変換してハードディスクコントローラ２８側に転送して、磁気ディスク媒体に書き込む。

ステップＳ４：リードアクセスか否かチェックし、リードコマンドによるリードアクセスであればステップ５に進み、そうでなければステップＳ６に進む。

ステップＳ５：ハードディスクコントローラから出力された暗号化されているリードデータを暗号鍵の鍵コード「ａ１～ａｎ」を使用して解読して、ホストインタフェース３０からホスト１１に転送される。

ステップＳ６：暗号鍵変更コマンドの受信をチェックしており、コマンドを受信するとステップＳ７に進み、そうでなければステップＳ２に戻る。

ステップＳ７：不揮発メモリから暗号鍵の鍵コード「ａ１～ａｎ」を読み出す。

ステップＳ８：ホスト１１から受信した暗号鍵変更コマンド（特殊コマンド）により不揮発メモリの暗号鍵の鍵コード「ａ１～ａｎ」を別の暗号鍵となる鍵コード、例えば鍵コード「ｂ１～ｂｎ」に変更する。この暗号鍵の変更は

（１）暗号鍵変更コマンドに付加された暗号鍵へ変更、

（２）現在に暗号鍵をシャッフルなどにより処理して別の暗号鍵へ変更、

となる。

ステップＳ９：不揮発メモリの暗号鍵を変更した暗号鍵に書き替える。

【００５９】

尚、ステップＳ８の暗号鍵の変更処理におけるシャッフルとしては変更前の暗号鍵の鍵コード「ａ１～ａｎ」に対し、ランダムにビットを反転をしたり、例えばバイト単位に分割して位置を入れ替えたり、更にはバイト分割をして位置を入れ替えて元の鍵コードとの排他論理和をとるなど適宜のシャッフルが適用できる。即ち、本発明における暗号鍵の変更は、変更前の暗号鍵が失われ、変更前とは異なる新たな変更鍵ができるものであれば変更の手法は問わない。

【００６０】

図６は、本発明の磁気ディスク装置に対する暗号鍵変更ツールを提供するネットワーク環境の説明図である。図６において、本発明の磁気ディスク装置１０を搭載したユーザコンピュータ６０を廃棄させる場合、ユーザコンピュータ（ホスト）６０のWWWブラウザ６２を使用して、インターネット６６上の例えば製造

元サーバ６４から暗号鍵変更用のツールをダウンロードして実行させることができる。

【００６１】

このため製造元サーバ６４には，WWWサーバ６８、ＨＤＤ廃棄管理部７０、ユーザ管理ファイル７２及び暗号鍵変更アプリケーションファイル７４が設けられている。

【００６２】

図７は、図６のユーザ管理ファイル７２の一例であり、管理ＩＤ、コンピュータ番号、ハードディスク番号をコンピュータの製造段階で作成して登録しており、更に暗号鍵変更フラグが設けられ、変更がなければフラグは０であり、ユーザからの要求で暗号鍵変更アプリケーションファイル７４からの暗号鍵変更ツールのダウンロードによる変更が行われるとフラグは１にセットされる。

【００６３】

この例では管理ＩＤが「０３０００００４」について暗号鍵変更フラグが「１」にセットされて暗号鍵変更処理が行われたことが示されており、このコンピュータは廃棄されるか、別のユーザにより再利用されていることになる。

【００６４】

図８は、図６の製造元サーバ６４にユーザコンピュータ６０のWWWブラウザ６２でアクセスした際に表示されるハードディスク廃棄ツール操作画面７５の説明図である。

【００６５】

このハードディスク廃棄ツール操作画面７５において、「ハードディスク廃棄ツールをインストールしますか」の表示に対し、「はい」のチェックボックスをクリックしてＯＫボタン７７を操作するとユーザコンピュータ６０において製造元サーバからダウンロードされたハードディスク廃棄ツールが実行され、磁気ディスク装置１０に記憶している暗号鍵を変更するための特殊コマンドが発行され、暗号鍵の変更が行われる。

【００６６】

このようにして一度磁気ディスク装置１０の暗号鍵を変更してしまうと、変更

後にユーザコンピュータ６０の電源を落として停止し、再度電源を投入したときには暗号鍵が変更されているため、その時、磁気ディスク媒体に記憶しているＯＳを含む全データは変更後の暗号鍵で解読されることとなり、暗号鍵が違うことにより全く無意味なデータが解読されることになり、結果として磁気ディスク装置の読出しによるＯＳの立上りはできず、ユーザコンピュータ６０はＯＳをインストールしていない全く未使用状態と同じ状態になる。

【００６７】

このためユーザコンピュータを廃棄した場合、第三者が廃棄されたユーザコンピュータを起動してもユーザコンピュータは全く動作せず、データの流出は起きない。

【００６８】

またユーザコンピュータを分解して磁気ディスク装置の暗号鍵を何らかの操作で入手したとしても、磁気ディスク媒体に記憶されているデータはすでに失われている変更前の暗号鍵により暗号化されたデータであり、この時、取得した暗号鍵によっては復元することはできず、変更後の暗号鍵がわかったとしてもデータの流出することはない。

【００６９】

一方、暗号鍵の変更を実行して廃棄したユーザコンピュータを別のユーザが再利用する際には、全く使用されていない新品のコンピュータと同様、ＯＳのインストールを行って磁気ディスク媒体の暗号化されたＯＳを記憶すれば、それ以降の処理は変更後の暗号鍵に従った暗号化と復元化が行われ、通常の暗号化処理を行ってないユーザコンピュータと同等に利用することができる。

【００７０】

また図６のようなネットワーク上からハードディスク廃棄ツールを取得してユーザコンピュータ６０に搭載している磁気ディスク装置１０の暗号鍵を変更することができるため、ユーザにおいて暗号鍵の管理は一切必要なく、ユーザコンピュータ６０を廃棄する際のひとつの手順としてネットワーク上からハードディスク廃棄ツールを取得してそれを実行すればよい。

【００７１】

このようなハードディスク廃棄ツールをユーザに提供する別の手法としてフロッピーディスク（Ｒ）などに格納してユーザに提供することも可能であるが、この場合、ネットワーク上から取得するほうが媒体の管理を必要としない分、簡単かつ確実に利用できる。

【００７２】

図９は、装置内の物理的な操作により暗号鍵を変更する本発明の他の実施形態にブロック図である。この実施形態にあっては暗号処理部４０に対し磁気ディスク装置内に変更操作部位７６を設けている。変更操作部位７６としては図２及び図３におけるコントロールボード１４上に設けているディップスイッチ、信号入力ピン、切断により操作入力を行うジャンパ線など、適宜の物理的な操作部位を用いることができる。

【００７３】

変更操作部位７６の物理的な操作が行われると、暗号鍵変更部５８に対しイベント入力が行われ、このイベント入力は暗号鍵変更部５８を動作する特殊コマンドと同等の機能をもっており、これにより暗号鍵変更部５８は暗号鍵記憶部５０に記憶している暗号鍵４２の鍵コード「ａ１～ａｎ」を例えば「ｂ１～ｂｎ」といった別の鍵コードに変更する。

【００７４】

この場合の鍵コードの変更は別の暗号鍵の鍵コードを予め記憶しておくことは安全でないことから、変更前の暗号鍵の鍵コード「ａ１～ａｎ」をシャッフルなどの動作により別の鍵コードに変更する暗号鍵の変更が望ましい。

【００７５】

図１０は、暗号鍵を磁気ディスク媒体に格納した本発明の他の実施形態のブロック図である。図１０において、暗号鍵４２は磁気ディスク媒体２０－１におけるユーザ記憶領域以外の記録領域、具体的には磁気ディスク装置の製造段階で各種のパラメータの格納に使用するいわゆるシステム領域に暗号鍵４２を記憶している。

【００７６】

このような磁気ディスク媒体２０－１に対する暗号鍵４２の格納に対応して暗

号処理部４０は暗号鍵読出書込部７８が設けられている。暗号鍵読出書込部７８は磁気ディスク装置をパワーオンスタート時にリードデータ処理部４８を介して磁気ディスク媒体２０－１のシステム領域に格納されている暗号鍵４２を読み出して、暗号エンコード部５４及び暗号デコード部５６に設定する。

【００７７】

またこの実施形態ではホストインタフェース３０を介してホスト１１側より暗号鍵変更のための特殊コマンドが与えられると、暗号鍵変更部５８は暗号鍵読出書込部７８のリード動作により磁気ディスク媒体２０－１から暗号鍵４２を読出し、これを変更後の暗号鍵に書き替え、ライトデータ処理部４６から磁気ディスク媒体２０－１のシステム領域に書き込んで暗号鍵を変更する。

【００７８】

図１１は、図１０と同じ暗号鍵を磁気ディスク媒体に格納する場合について暗号鍵の変更を装置内の変更操作部位７６により行う本発明の他の実施形態のブロック図である。

【００７９】

この場合の変更操作部位７６は、図９の実施形態と同様、図２及び図３のコントロールボード１４側に設けられたディップスイッチ、信号入力ピン、切断により操作入力を行うジャンパ線などの適宜の物理的な操作部位が用いられている。

【００８０】

尚、上記の実施形態にあっては、暗号処理部４０をホストインタフェース３０とハードディスクコントローラ２８の間に設けてデータにの暗号化と復号を実行しているが、暗号処理部４０をハードディスクコントローラ２８とリードライトＬＳＩ２６の間に設け、磁気ディスク媒体に対する記憶読出しのためのフォーマット済みのデータに対し、暗号処理を行うようにしても良い。

【００８１】

即ち本発明にあっては磁気ディスク媒体に記憶する前であれば適宜の段階で暗号化しても良く、また磁気ディスク媒体からの読出しについても読出し後のデータがあれば適宜の位置で暗号データの復元を行ってもよい。

【００８２】

また本発明はその目的と利点を損なわない適宜の変形を含み、更に上記の実施形態に示した数値による限定は受けない。

【００８３】

ここで本発明の特徴を列挙すると次の付記のようになる。

（付記）

（付記1）

データの暗号化と復元に使用する暗号鍵を記憶した暗号鍵記憶部と、

インタフェースを介して上位装置から入力されたデータを前記暗号鍵を用いて暗号化して記録媒体に記録させる暗号エンコード部と、

前記記録媒体から読み出された暗号データを前記暗号鍵を用いて復元して前記インタフェースより上位装置にデータを出力させる暗号デコード部と、

前記暗号鍵記憶部に記憶されている暗号鍵を変更する暗号鍵変更部と、

を備えたことを特徴とする磁気ディスク装置。（１）

【００８４】

（付記２）

付記1記載の磁気ディスク装置に於いて、前記暗号鍵記憶部は、装置の製造段階で書き込まれた所定の暗号鍵を記憶することを特徴とする磁気ディスク装置。

【００８５】

（付記３）

付記１記載の磁気ディスク装置に於いて、前記暗号鍵記憶部は不揮発メモリであることを特徴とする磁気ディスク装置。

【００８６】

（付記４）

付記１記載の磁気ディスク装置に於いて、前記暗号鍵記憶部は記録媒体のユーザ記録領域以外の媒体領域であることを特徴とする磁気ディスク装置。

【００８７】

（付記５））

付記1記載の磁気ディスク装置に於いて、前記暗号鍵変更部は、前記記録媒体上のユーザ記録領域に存在する全ての記録データを一括して破棄する際に、前記

暗号鍵記憶部に記憶されている暗号鍵を変更することを特徴とする磁気ディスク装置。（２）

【００８８】

（付記６）

付記1記載の磁気ディスク装置に於いて、前記暗号鍵変更部は、上位装置のコマンド体系以外の特殊コマンドにより、前記暗号鍵記憶部の暗号鍵を変更することを特徴とする磁気ディスク装置。（３）

【００８９】

（付記７）

付記1記載の磁気ディスク装置に於いて、前記暗号鍵変更部は、前記上位装置にインストールされた暗号鍵変更アプリケーションからの特殊コマンドにより、前記暗号鍵記憶部の暗号鍵を変更することを特徴とする磁気ディスク装置。

【００９０】

（付記８）

付記1記載の磁気ディスク装置に於いて、前記暗号鍵変更部は、前記上位装置がネットワークを介してインストールした暗号鍵変更アプリケーションからの特殊コマンドにより、前記暗号鍵記憶部の暗号鍵を変更することを特徴とする磁気ディスク装置。

【００９１】

（付記９）

付記1記載の磁気ディスク装置に於いて、前記暗号鍵変更部は、装置内における物理的なイベント操作を認識して、前記暗号鍵記憶部の暗号鍵を変更することを特徴とする磁気ディスク装置。

【００９２】

（付記１０）

付記1記載の磁気ディスク装置に於いて、前記暗号鍵変更部は、前記暗号鍵記憶部に記憶されている暗号鍵の掻き混ぜ等の処理のより新たな暗号鍵を生成して変更することを特徴とする磁気ディスク装置。

【００９３】

（付記１１）

付記1記載の磁気ディスク装置に於いて、前記暗号鍵変更部は、前記暗号鍵記憶部に記憶されている暗号鍵を、上位装置からの暗号鍵変更コマンドに付加された別の暗号鍵に変更することを特徴とする磁気ディスク装置。

【００９４】

（付記１２）

磁気ディスク装置の暗号処理方法に於いて、

データの暗号化と復号に使用する暗号鍵を記憶部に記憶する暗号鍵記憶ステップと、

インタフェースを介して上位装置から入力されたデータを前記暗号鍵を用いて暗号データに変換して記録媒体に記録させる暗号化記録ステップと、

前記記録媒体から読み出された暗号データを前記暗号鍵を用いて復元して前記インタフェースより上位装置にデータを出力させる復元読出ステップと、

前記暗号鍵記憶部に記憶されている暗号鍵を変更する暗号鍵変更ステップと、

を備えたことを特徴とする磁気ディスク装置の暗号処理方法。（４）

【００９５】

（付記１３）

付記１２記載の磁気ディスク装置の暗号処理方法に於いて、前記暗号鍵変更ステップは、前記記録媒体上のユーザ記録領域に存在する全ての記録データを一括して破棄する際に、前記暗号鍵記憶部に記憶されている暗号鍵を変更することを特徴とする磁気ディスク装置の暗号処理方法。

【００９６】

（付記１４）

磁気ディスク装置に内蔵されたコンピュータに、

データの暗号化と復号に使用する暗号鍵を記憶部に記憶する暗号鍵記憶ステップと、

インタフェースを介して上位装置から入力されたデータを前記暗号鍵を用いて暗号データに変換して記録媒体に記録させる暗号化記録ステップと、

前記記録媒体から読み出された暗号データを前記暗号鍵を用いて復元して前記イ

ンタフェースより上位装置にデータを出力させる復元読出ステップと、
前記暗号鍵記憶部に記憶されている暗号鍵を変更する暗号鍵変更ステップと、
を実行させることを特徴とするプログラム。（５）

【００９７】

（付記１５）

付記１４記載のプログラムに於いて、前記暗号鍵変更ステップは、前記記録媒体上のユーザ記録領域に存在する全ての記録データを一括して破棄する際に、前記暗号鍵記憶部に記憶されている暗号鍵を変更することを特徴とするプログラム。

【００９８】

【発明の効果】

以上説明してきたように本発明によれば、磁気ディスク装置内に記憶保持している暗号鍵を変更するだけで記憶媒体上のデータを破棄することができ、時間のかかる記憶媒体のデータ領域の全面消去を行うことなく、データの流出が確実に防止でき、データの破棄を容易に行うことができる。

【００９９】

また本発明にあっては装置内、例えばインタフェース部分で書込みの際のデータの暗号化と読出しの際の暗号データを復元を行うため、インタフェースの外側に位置するホスト側は本発明の磁気ディスク装置における暗号処理を意識する必要なく、従来の磁気ディスク装置と同等に扱うことができ、本発明の磁気ディスク装置は暗号処理を内蔵していても従来の磁気ディスク装置と同等に置き換えができる。

【０１００】

また暗号鍵を変更して破棄された本発明の磁気ディスク装置の不揮発メモリあるいは記憶媒体より暗号鍵を取り出して記憶媒体のデータを読み出した場合にあっても、記憶媒体のデータは変更前の暗号鍵で暗号化されたデータであり、取り出した暗号鍵は変更後であるため、暗号鍵を使用しても記憶媒体の暗号データは復元できず、データの安全性が完全に保証される。

【０１０１】

また本発明の磁気ディスク装置は暗号化されたデータと暗号鍵を装置内に格納しているため、ユーザは通常の使用において暗号鍵を管理する必要がなく、暗号鍵に対するユーザの負担は生じない。

【０１０２】

更に暗号鍵を変更すると磁気ディスク装置が未使用状態に戻ることとなり、ホストにおけるＯＳのインストールにより再使用ができる。

【図面の簡単な説明】

【図１】

本発明の原理説明図

【図２】

ハードウェアで暗号処理を行う本発明による磁気ディスク装置のブロック図

【図３】

プログラムで暗号処理を行う本発明による磁気ディスク装置のブロック図

【図４】

本発明によるプログラム暗号処理の機能構成のブロック図

【図５】

本発明における暗号処理のフローチャート

【図６】

本発明の磁気ディスク装置に対し暗号鍵変更ツールを提供するネットワーク環境の説明図

【図７】

図６の製造元サーバにおけるユーザ管理ファイルの説明図

【図８】

図６のブラウザにインストールしたハードディスク廃棄ツールの操作画面の説明図

【図９】

装置内の変更操作部位により暗号鍵を変更する本発明の他の実施形態のブロック

図

【図１０】

暗号鍵を記録媒体に格納した本発明の他の実施形態のブロック図

【図１１】

暗号鍵を記録媒体に格納し装置内の変更操作部位により暗号鍵を変更する本発明の他の実施形態のブロック図

【符号の説明】

１０：ハードディスクドライブ（ＨＤＤ）

１１：ホスト

１２：ディスクアッセンブリィ

１４：コントロールボード

１６：スピンドルモータ（ＳＰＭ）

１８：ボイスコイルモータ（ＶＣＭ）

２０，２０－１，２０－２：磁気ディスク媒体

２２－１～２２－４：ヘッド

２４：ヘッドＩＣ

２６：リードライトＬＳＩ

２８：ハードディスクコントローラ（ＨＤＣ）

３０：ホストインタフェース

３２：ＳＤＲＡＭ

３４：ＭＰＵ

３６：フラッシュＲＯＭ

３８：ＶＣＭ／ＳＰＭコントローラ

４０：暗号処理部

４２：暗号鍵

４４：スクランブル回路

４６：ライトデータ処理部

４８：リードデータ処理部

５０：暗号鍵記憶部

５２：暗号鍵設定部

５４：暗号エンコード部

５６：暗号デコード部

５８：暗号鍵変更部

６０：ユーザコンピュータ

６２：WWWブラウザ

６４：製造元サーバ

６６：インターネット

６８：WWWサーバ

７０：ＨＤＤ廃棄管理部

７２：ユーザ管理ファイル

７５：ハードディスク廃棄ツール操作画面

７４：暗号鍵変更アプリケーションファイル

７６：変更操作部位

７７：ＯＫボタン

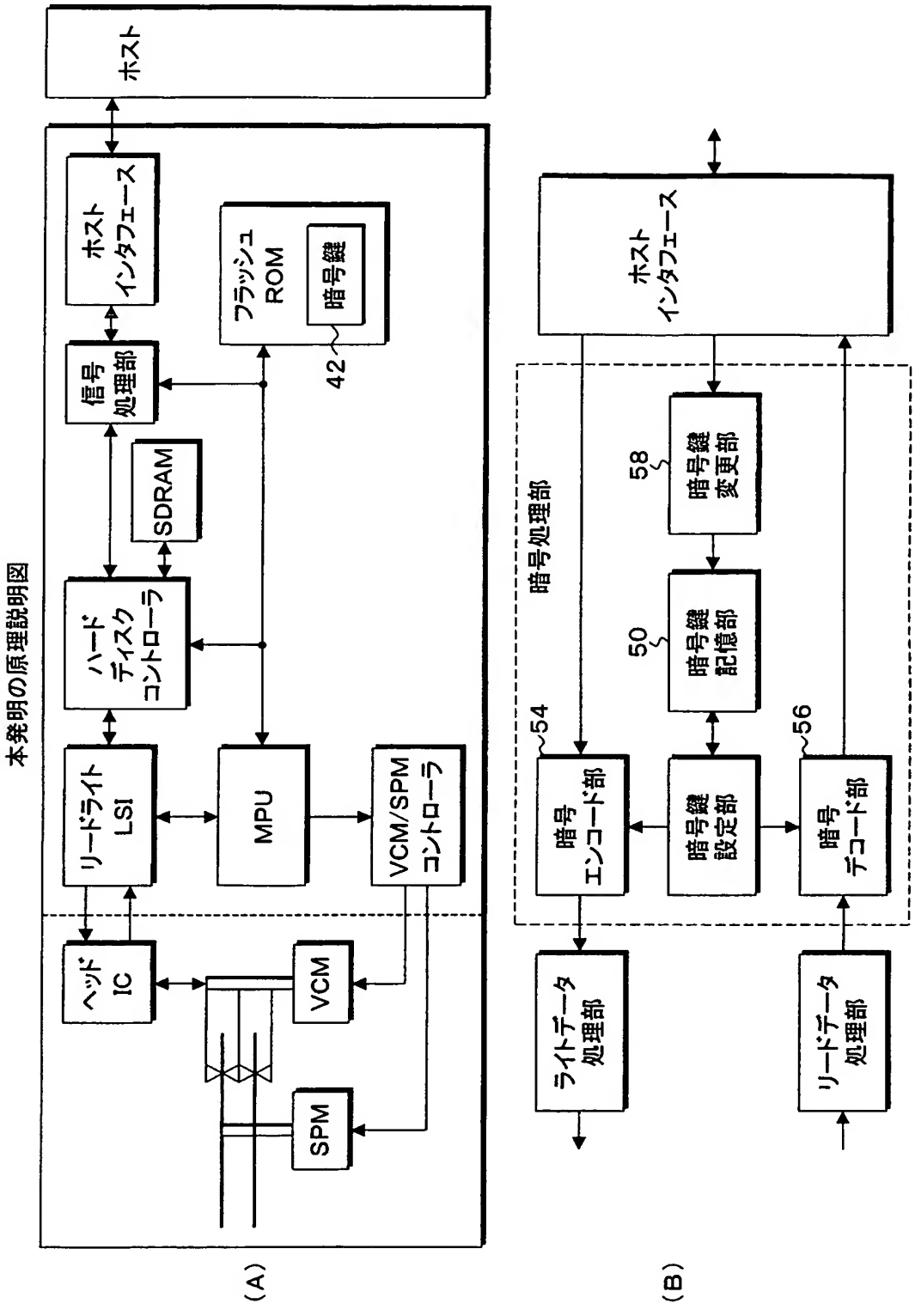
７８：暗号鍵読出書込部

８０：ライトヘッド

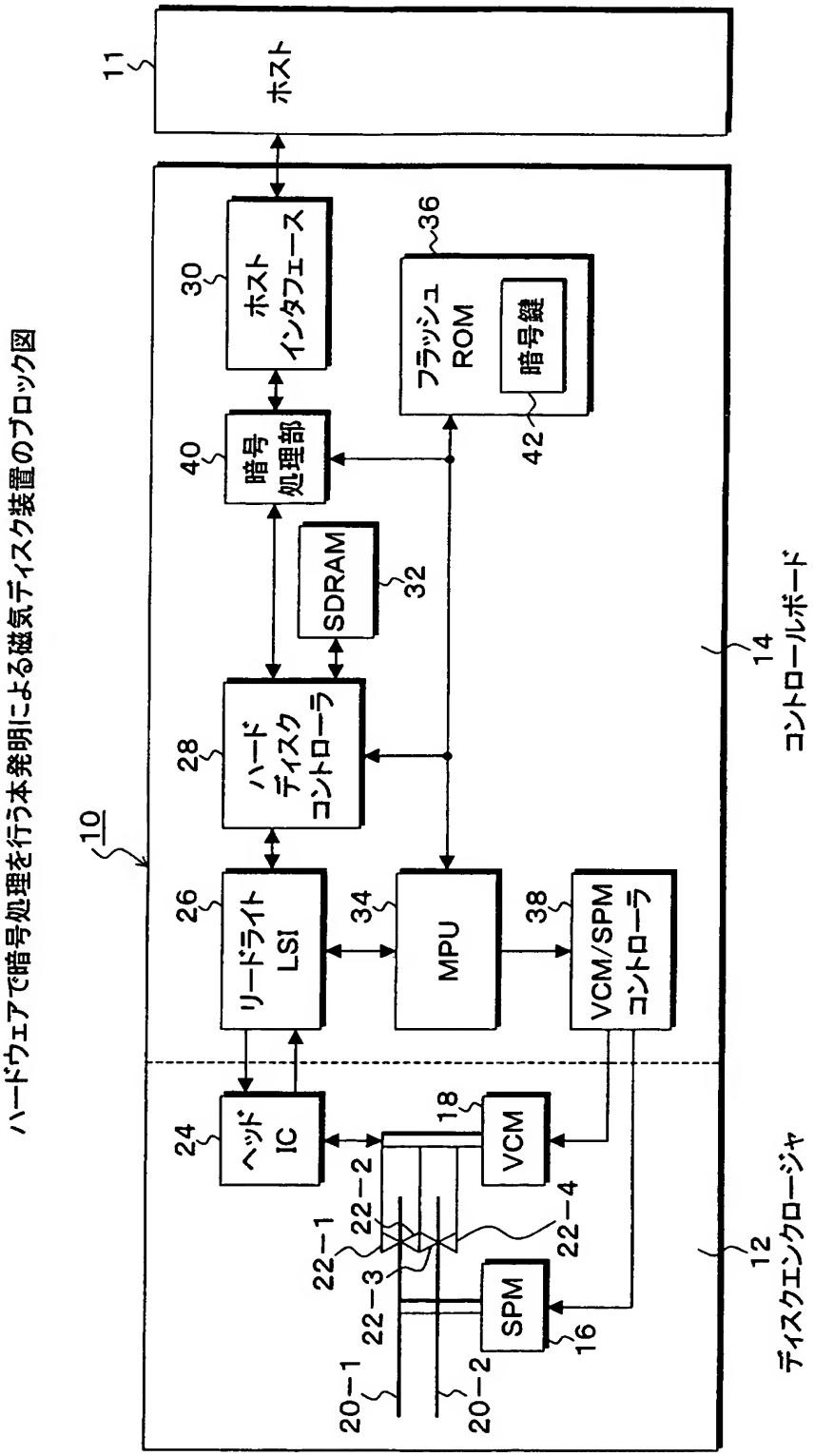
８２：リードヘッド

【書類名】　　図面

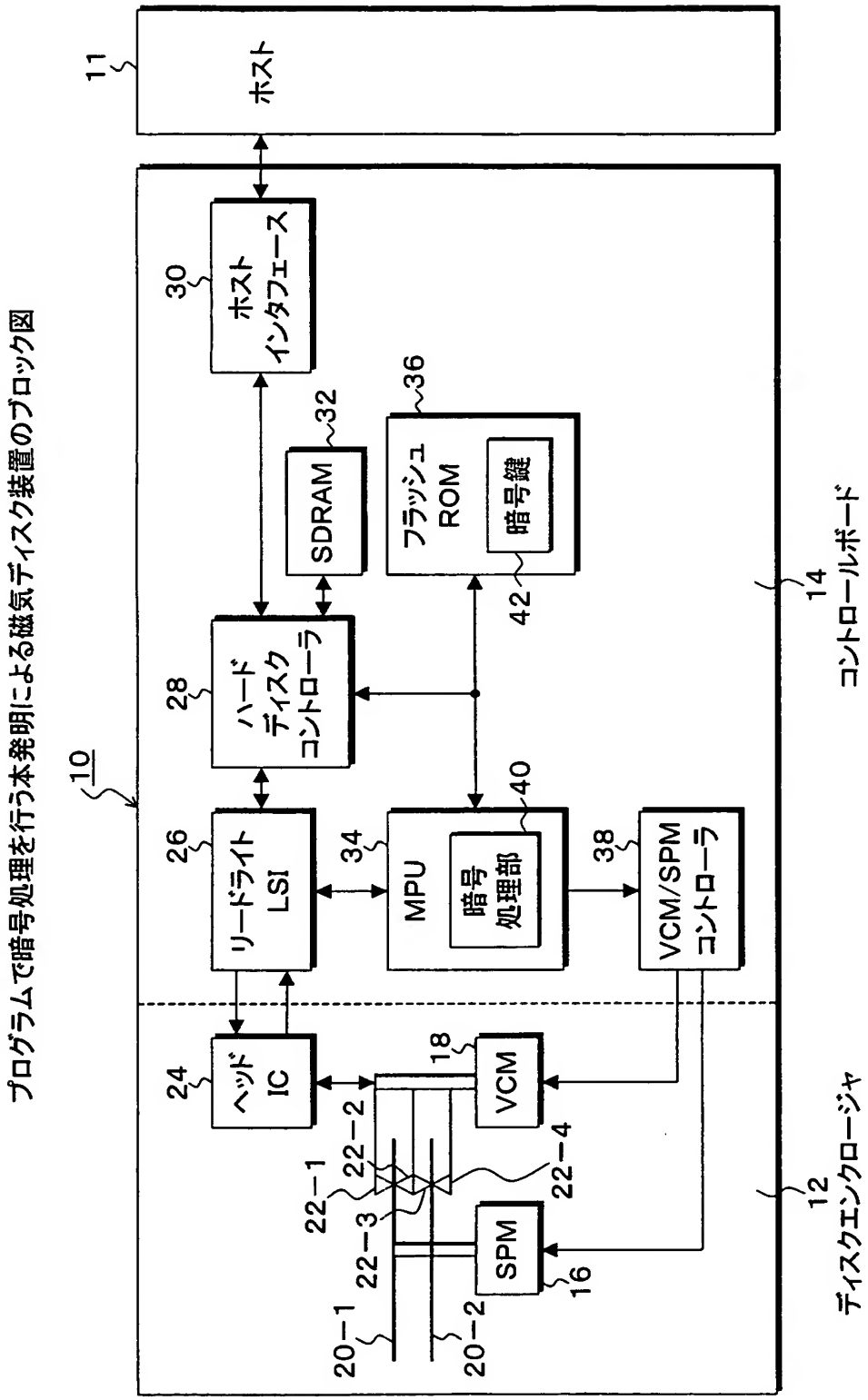
【図１】


本発明の原理説明図
ホスト
ホスト
インタフェース
信号
処理部
フラッシュ
ROM
暗号鍵
42
SDRAM
ハード
ディスク
コントローラ
リードライト
LSI
MPU
VCM/SPM
コントローラ
ヘッド
IC
VCM
SPM
(A)
ホスト
インタフェース
暗号処理部
58
暗号鍵
変更部
50
暗号鍵
記憶部
54
暗号
エンコード部
暗号鍵
設定部
56
暗号
デコード部
ライトデータ
処理部
リードデータ
処理部
(B)

【図２】

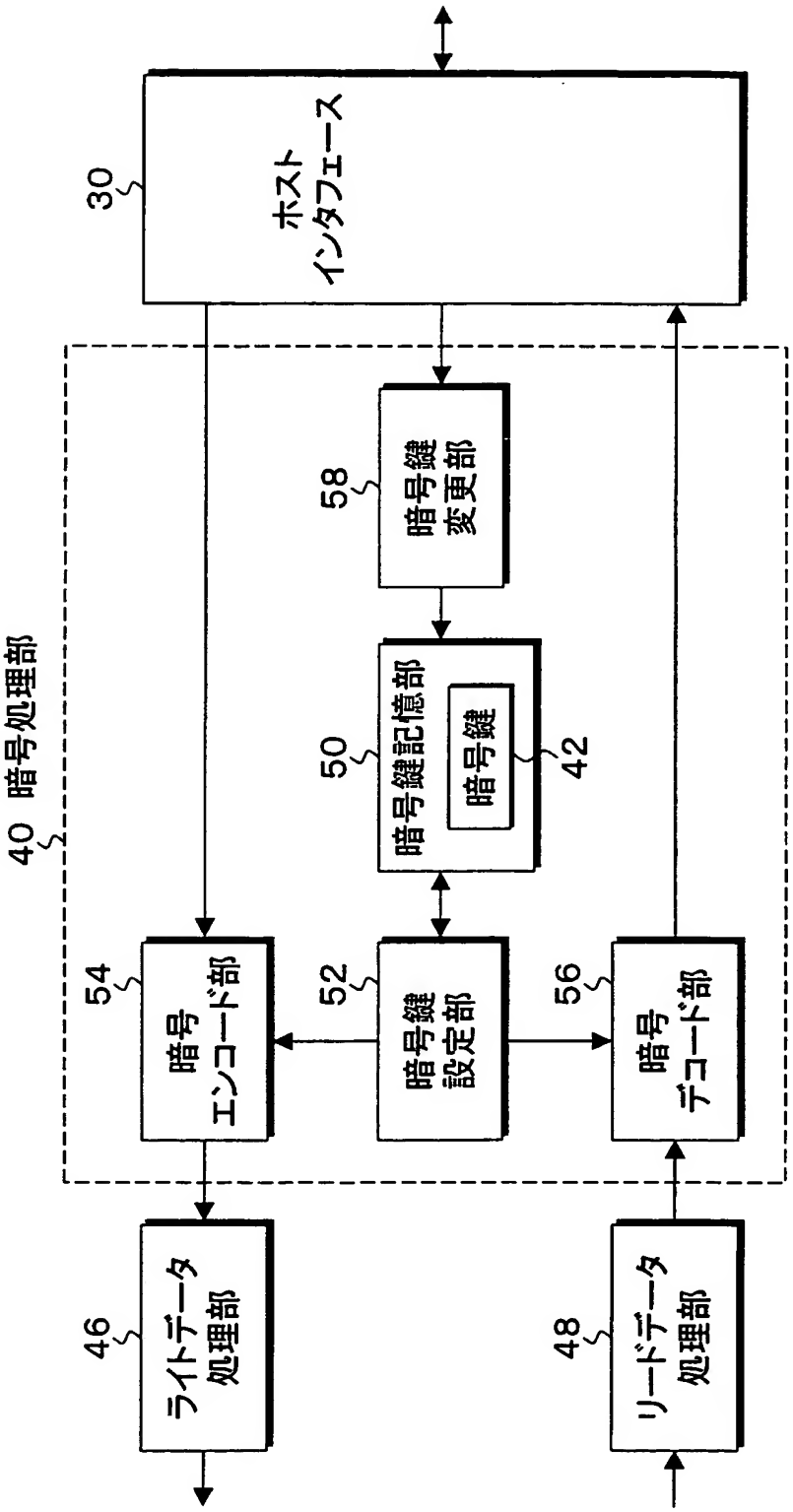

ハードウェアで暗号処理を行う本発明による磁気ディスク装置のブロック図
11
ホスト
30
ホスト
インタフェース
36
フラッシュ
ROM
暗号鍵
42
40
暗号
処理部
SDRAM
32
28
ハード
ディスク
コントローラ
10
26
リードライト
LSI
34
MPU
38
VCM/SPM
コントローラ
14
コントロールボード
24
ヘッド
IC
18
VCM
22−2
22−1
22−4
22−3
SPM
16
20−1
20−2
12
ディスクエンクロージャ

【図３】


プログラムで暗号処理を行う本発明による磁気ディスク装置のブロック図
11
ホスト
10
30
ホスト
インタフェース
32
SDRAM
36
フラッシュ
ROM
暗号鍵
42
28
ハード
ディスク
コントローラ
14
コントロールボード
26
リードライト
LSI
34
MPU
暗号
処理部
40
38
VCM/SPM
コントローラ
24
ヘッド
IC
18
VCM
22－1
22－2
22－3
22－4
SPM
16
20－1
20－2
12
ディスクエンクロージャ

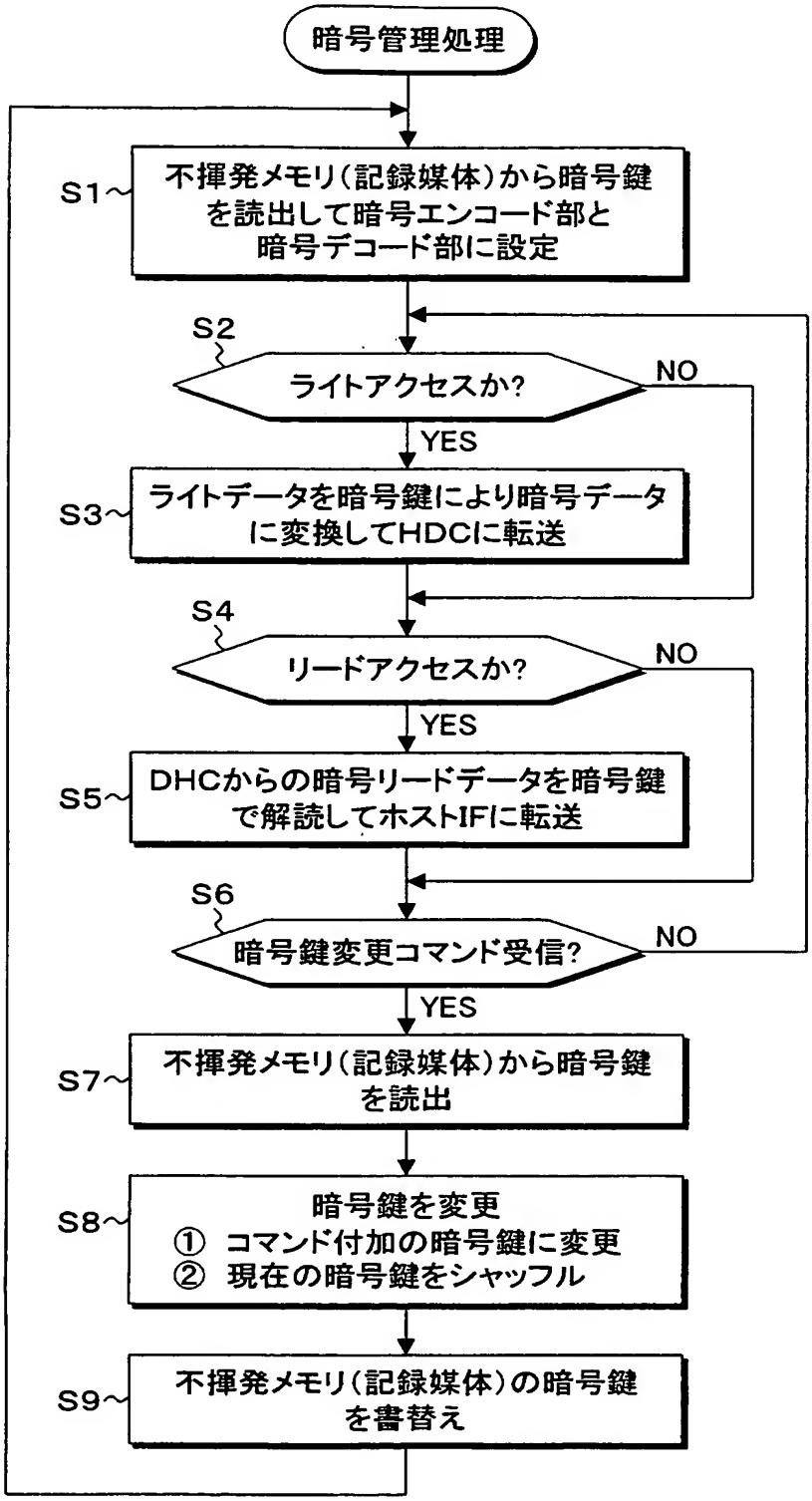
【図４】

本発明によるプログラム暗号処理の機能構成のブロック図



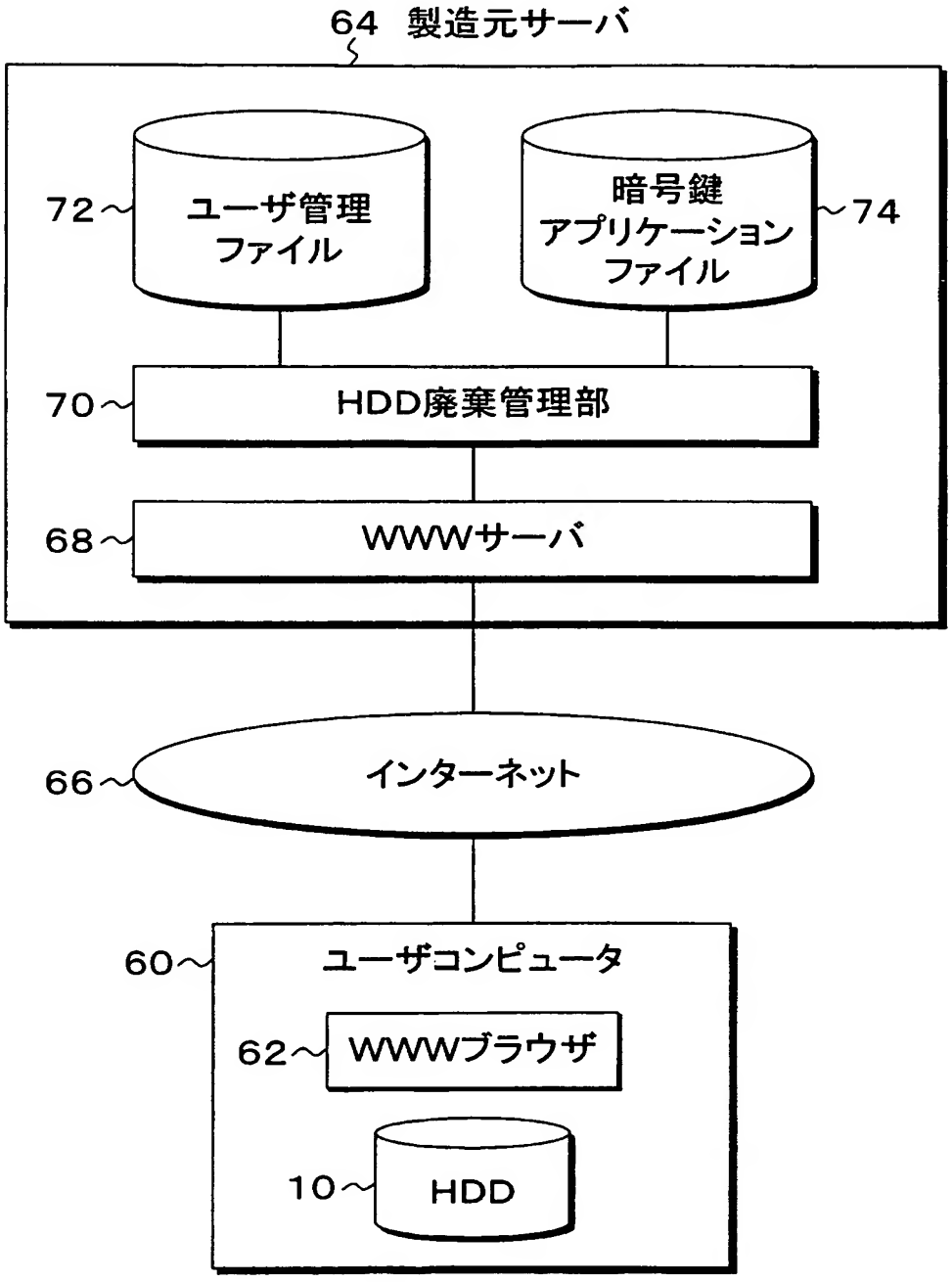
【図５】

本発明における暗号処理のフローチャート



【図６】

本発明の磁気ディスク装置に対し暗号鍵変更ツールを提供するネットワーク環境の説明図



【図７】

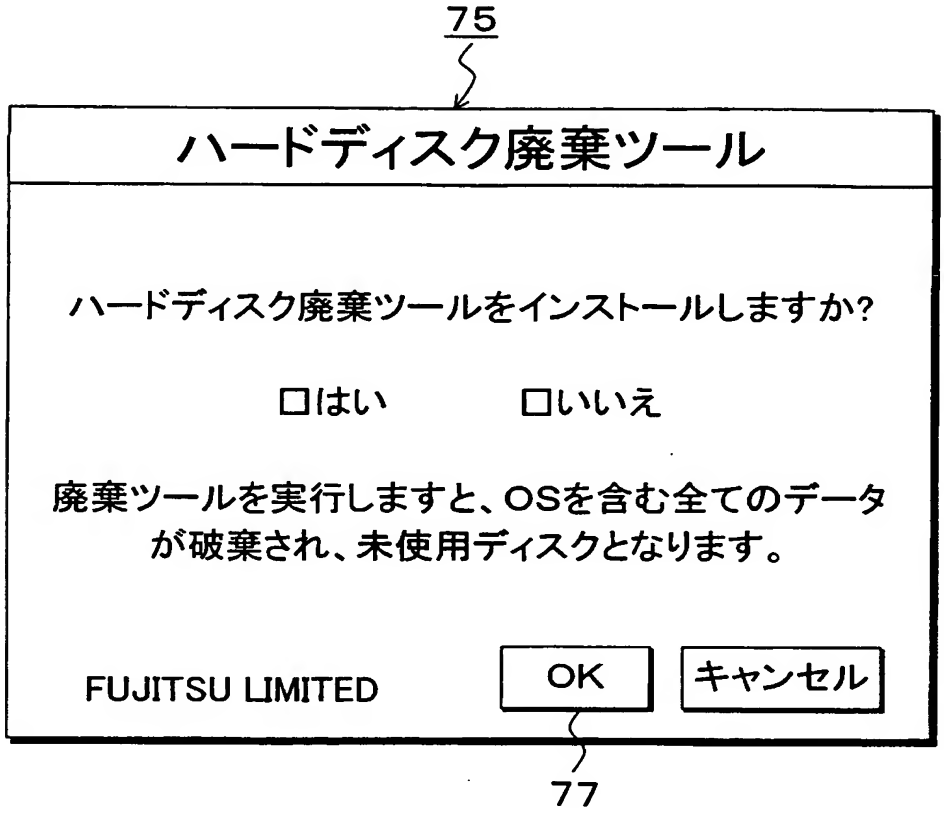
図6の製造元サーバにおけるユーザ管理ファイルの説明図

72

管理ID	コンピュータ番号	ハードディスク番号	暗号鍵変更フラグ
0300001	FJ1234567890	HDD0000000100	0
0300002	FJ1234567891	HDD0000000101	0
0300003	FJ1234567892	HDD0000000102	0
0300004	FJ1234567893	HDD0000000103	1
0300005	FJ1234567894	HDD0000000104	0
0300006	FJ1234567895	HDD0000000105	0

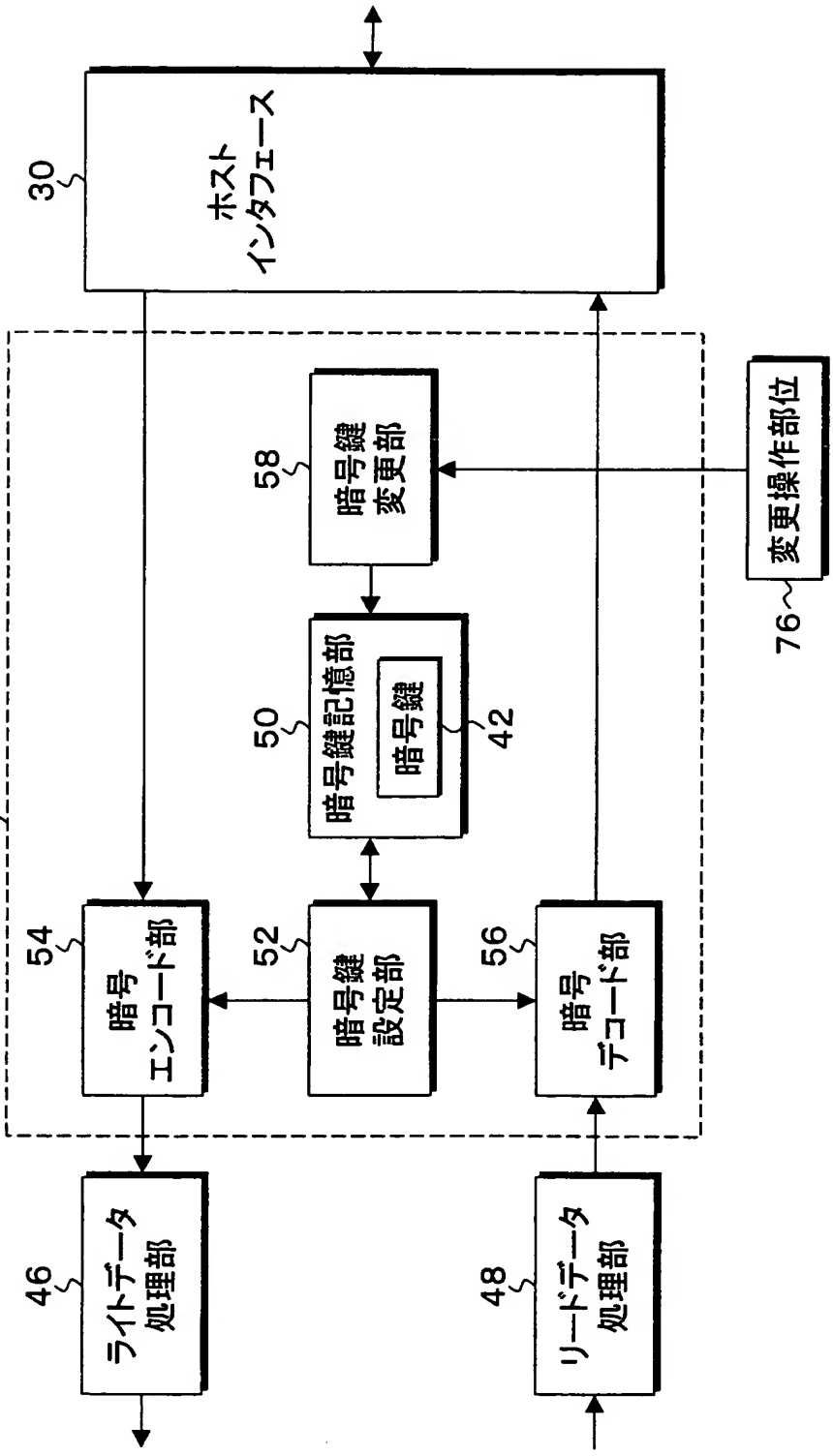
【図８】

図6のブラウザにインストールしたハードディスク廃棄ツールの操作画面の説明図



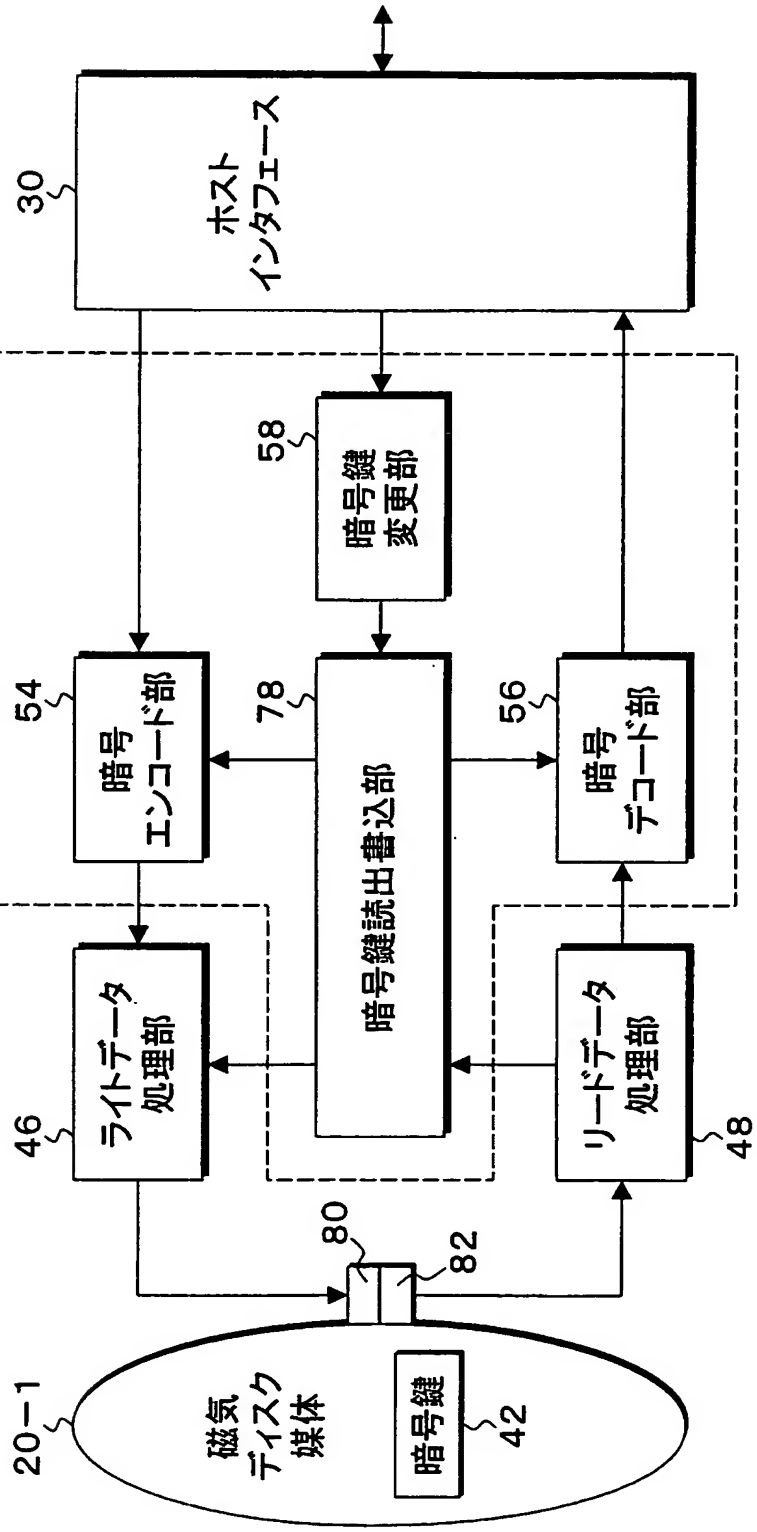
【図９】

装置内の変更操作部位により暗号鍵を変更する本発明の他の実施形態のブロック図



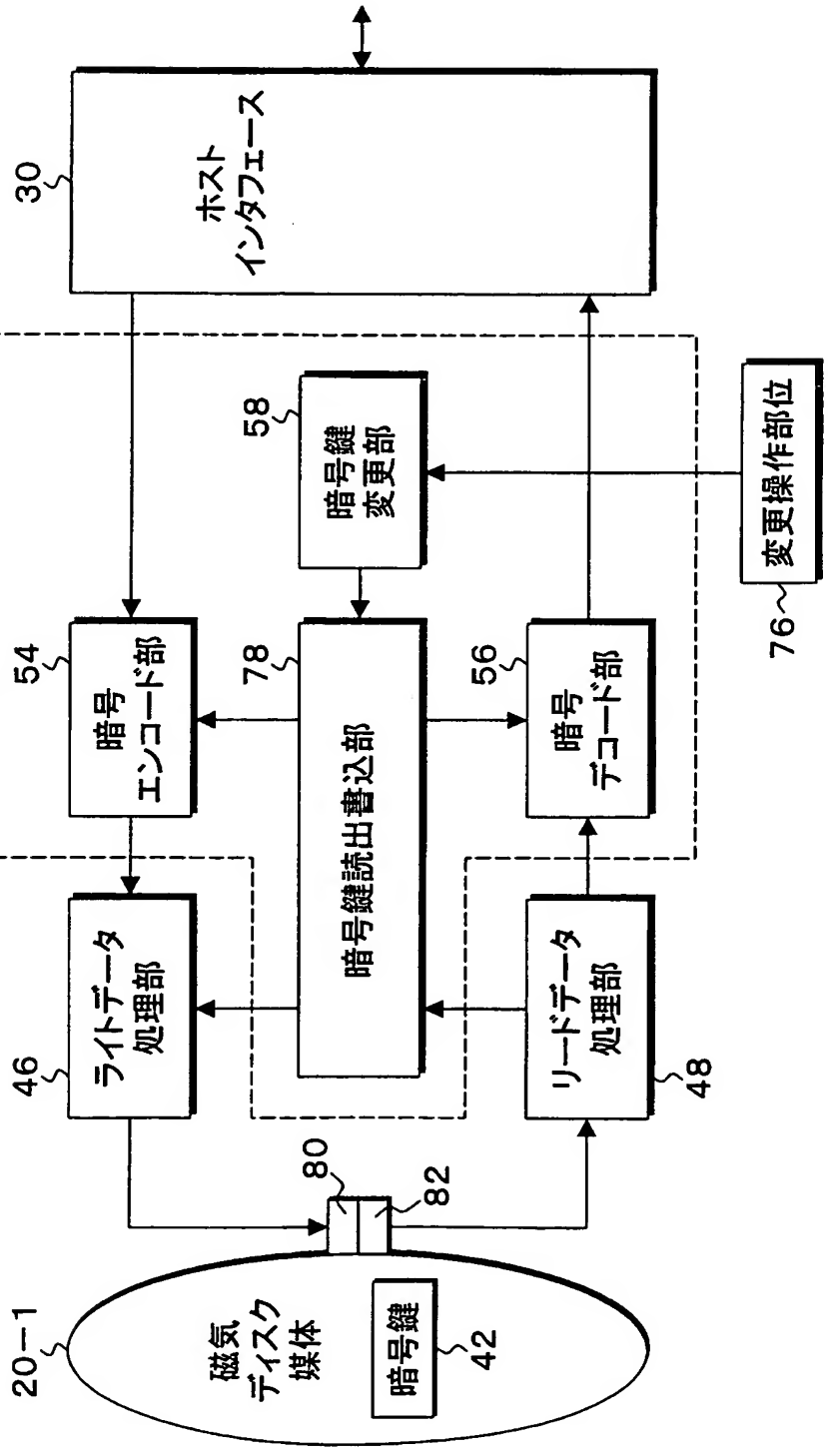
【図１０】

暗号鍵を記録媒体に格納した本発明の他の実施形態のブロック図



【図１１】

暗号鍵を記録媒体に格納し装置内の変更操作部位により暗号鍵を変更する本発明の他の実施形態のブロック図



【書類名】　　要約書

【要約】

【課題】暗号化技術を利用して簡単且つ確実にデータ流出を防止する。

【解決手段】　暗号鍵記憶部５０にデータの暗号化と復元に使用する暗号鍵４２を記憶させる。暗号エンコード部５４はホストインタフェース３０を介して上位装置から入力されたデータを暗号鍵４２を用いて暗号化して記録媒体に記録させる。暗号デコード部５６は記録媒体から読み出された暗号データを暗号鍵４２を用いて復元してホストインタフェース３０より上位装置にデータを出力させる。磁気ディスク装置を廃棄する際には、暗号鍵変更部５８により暗号鍵記憶部５０に記憶されている暗号鍵４２を変更して復元不能とする。

【選択図】　　図１

特願２００３－１３６８６７

出　願　人　履　歴　情　報

識別番号　　［０００００５２２３］

１．変更年月日　　１９９６年　３月２６日
［変更理由］　　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社